ON THE ORDER OF STIRLING NUMBERS AND ALTERNATING BINOMIAL COEFFICIENT SUMS

Ira M. Gessel*

Department of Mathematics, Brandeis University, Waltham, MA 02454

and

Tamás Lengyel

Occidental College, 1600 Campus Road, Los Angeles, CA 90041

June 2000

1. INTRODUCTION

We prove that the order of divisibility by prime p of $k!\,S(a\,(p-1)\,p^q,k)$ does not depend on a and q if q is sufficiently large and k/p is not an odd integer. Here $S(n,k)$ denotes the Stirling number of the second kind; i.e., the number of partitions of a set of n objects into k nonempty subsets. The proof is based on divisibility results for p-sected alternating binomial coefficient sums. A fairly general criterion is also given to obtain divisibility properties of recurrent sequences when the coefficients follow some divisibility patterns.

The motivation of the paper is to generalize the identity [8]

$$\nu_2(k!\,S(n,k)) = k-1, \quad 1 \le k \le n, \tag{1}$$

where $S(n,k)$ denotes the Stirling number of the second kind, and $n = a\,2^q, a$ is odd, and q is sufficiently large (for example, $q \ge k-2$ suffices). Here $\nu_p(m)$ denotes the order of divisibility by prime p of m, i.e., the greatest integer e such that p^e divides m. It is worth noting the remarkable fact that the order of divisibility by 2 does not depend on a and q if q is sufficiently large. We will clarify later what value is large enough.

Our objective in this paper is to analyze $\nu_p(k!\,S(n,k))$ for an arbitrary prime p. It turns out that identity (1) can be generalized to calculate the exact value of $\nu_p(k!\,S(n,k))$ if $n = a\,(p-1)\,p^q$ and k is divisible by $p-1$. The main result of this paper is

Theorem 1: If $n = a\,(p-1)\,p^q$, $1 \le k \le n$, a and q are positive integers such that $(a,p)=1$, q is sufficiently large, and k/p is not an odd integer, then

$$\nu_p(k!\,S(n,k)) = \left\lfloor \frac{k-1}{p-1} \right\rfloor + \tau_p(k),$$

where $\tau_p(k)$ is a nonnegative integer. Moreover, if k is a multiple of $p-1$ then $\tau_p(k)=0$.

Here $\lfloor x \rfloor$ denotes the greatest integer function. Note that the order of divisibility by p of $k!\,S(a\,(p-1)\,p^q,k)$ does not depend on a and q if q is sufficiently large. For instance,

*partially supported by NSF grant DMS-9622456

we may choose q such that $q > \frac{k}{p-1} - 2$ in this case. Numerical evidence suggests that the condition on the magnitude of q may be relaxed and it appears that $n \geq k$ suffices in many cases (cf. [8]).

The case excluded by Theorem 1, in which k/p is an odd integer, behaves somewhat differently:

Theorem 2: For any odd prime p, if k/p is an odd integer then $\nu_p(k!\, S(a\,(p-1)\,p^q, k)) > q$.

In Section 2 we prove a fundamental lemma: If $n = a(p-1)p^q$ then

$$(-1)^{k+1} k!\, S(n,k) \equiv G_p(k) \pmod{p^{q+1}}, \tag{2}$$

where

$$G_p(k) = \sum_{p|i} \binom{k}{i} (-1)^i.$$

All of our divisibility results for the Stirling numbers are consequences of divisibility results for the alternating binomial coefficient sums $G_p(k)$, which are of independent interest. Theorem 2 is an immediate consequence of (2), since if k/p is an odd integer, the corresponding binomial coefficient sum is 0.

To prove Theorem 1, we prove the analogous divisibility result for $G_p(k)$. The proof is presented in Section 2, and it combines number-theoretical, combinatorial and analytical arguments. By an application of Euler's theorem, we prove (2). We then apply p-section of the binomial expansion of $(1-x)^k$ to express $G_p(k)$ as a sum of $p-1$ terms involving roots of unity. We take a closer look at this sum from different perspectives in Sections 3 and 4 and give a comprehensive study of the special cases $p = 3$ and 5. We choose two different approaches in these sections: we illustrate the use of roots of unity in the case in which $p = 3$, and for $p = 5$ we use known results relating $G_5(k)$ to Fibonacci and Lucas numbers.

We outline a generating function based method to analyze the sum in terms of a recurrent sequence in Section 2. A fairly general lemma (Lemma 7) is also given in order to provide the framework for proving divisibility properties. The reader may find it a helpful tool in obtaining divisibility properties of recurrent sequences when the coefficients follow some divisibility patterns (e.g., [1]). The lemma complements previous results that can be found, for example, in [11] and [13]. Theorem 1 follows by an application of Lemma 7. A similar approach yields

Theorem 3: For any odd prime p and any integer t,

$$\sum_{i \equiv t \pmod p} \binom{k}{i} (-1)^i \equiv \begin{cases} (-1)^{\frac{k}{p-1}-1} p^{\frac{k}{p-1}-1} & \pmod{p^{\frac{k}{p-1}}}, \text{ if } k \text{ is divisible by } p-1, \\ 0 & \pmod{p^{\lfloor \frac{k}{p-1} \rfloor}}, \text{ otherwise.} \end{cases}$$

Fleck [4] and Kapferer [7] proved the second part of Theorem 3, and Lundell [10] obtained the first part (Theorem 1.1 (ii)). Lundell has only indicated that the proof is based on a tedious induction on $\lfloor \frac{k}{p-1} \rfloor$. The case $t = 0$, $k = p(p-1)$ of Theorem 3 was proposed as an American Mathematical Monthly problem by Evans [3].

The proofs of Lemma 7 and Theorem 3 are given in Section 5 in which an application of Theorem 3 is also presented to prove its generalization:

Theorem 4: Let p be an odd prime and let m be an integer with $0 \le m \le \min(k, p)$ such that $r = \frac{k-m}{p-1}$ is an integer. We set $r \equiv r' \pmod{p}$ with $1 \le r' \le p$. If $r' \ge m$ then for any integer t,

$$\sum_{i \equiv t \pmod{p}} \binom{k}{i} (-1)^i i^m \equiv (-1)^{m+\frac{k-m}{p-1}-1} \binom{k}{m} m!\, p^{\frac{k-m}{p-1}-1} \pmod{p^{\frac{k-m}{p-1}+\nu_p\left(\binom{k}{m} m!\right)}}.$$

For example, it follows that $\sum_{i \equiv t \pmod{17}} \binom{135}{i}(-1)^i i^7 \equiv \binom{135}{7} 7!\, 17^7 \pmod{17^8}$, independently of t. Here we have $m = 7$ and $r' = r = 8$.

Theorem 4 is a generalization of Theorem 1.7 of [10]. Note that the conditions of Theorem 4 are always satisfied for $m = 0$ and 1 provided $p - 1 \mid k - m$. The theorem can be generalized to the case in which $p = 2$ and $m = 0$ or 1, also (see also [8]), e.g.,

$$\sum_{2 \mid i} \binom{k}{i} = \sum_{2 \nmid i} \binom{k}{i} = 2^{k-1}.$$

Some conjectures on $\tau_p(k)$ are discussed at the end of the paper.

2. TOOLS AND THE GENERAL CASE

Lemma 5: If $n = a(p-1)p^q$ then

$$(-1)^{k+1} k!\, S(n,k) \equiv \sum_{p \mid i} \binom{k}{i} (-1)^i \pmod{p^{q+1}}. \tag{3}$$

Proof: By a well-known identity for the Stirling numbers [2, p. 204], we have

$$k!\, S(n,k) = \sum_{i=0}^{k} \binom{k}{i} i^n (-1)^{k-i} \equiv \sum_{p \nmid i} \binom{k}{i} i^n (-1)^{k-i} \pmod{p^n}.$$

For $n = a\,(p-1)\,p^q$ and $(i,p) = 1$, we have

$$i^n \equiv 1 \pmod{p^{q+1}}$$

by Euler's theorem. Notice that $n \geq q+1$. By the binomial theorem, we obtain

$$(1-1)^k = \sum_{p|i} \binom{k}{i}(-1)^i + \sum_{p\not|i} \binom{k}{i}(-1)^i;$$

therefore we have

$$k!\, S(n,k) \equiv \sum_{p\not|i} \binom{k}{i}(-1)^{k-i} = (-1)^k \sum_{p\not|i} \binom{k}{i}(-1)^i$$
$$= (-1)^{k+1} \sum_{p|i} \binom{k}{i}(-1)^i \pmod{p^{q+1}}. \quad \blacksquare$$

Lemma 6: For any odd prime p, if k is an odd multiple of p then

$$\sum_{p|i} \binom{k}{i}(-1)^i = 0.$$

Proof: The terms $\binom{k}{i}(-1)^i$ and $\binom{k}{k-i}(-1)^{k-i}$ cancel in (3). $\blacksquare$

Theorem 2 is an immediate consequence of Lemmas 5 and 6. We note that by multisection identities ([12, p. 131] or [2, p. 84]),

$$\sum_{m|i} \binom{k}{i}(-1)^i = \frac{1}{m} \sum_{t=1}^{m-1} (1-\omega^t)^k, \tag{4}$$

where $\omega = \exp(2\pi i/m)$ is a primitive mth *root of unity.* To illustrate the use of this identity, we note that identity (1) follows immediately if we set $m = p = 2$: identities (3) and (4) with $\omega = -1$, imply that

$$k!\, S(n,k) \equiv (-1)^{k+1} 2^{k-1} \pmod{2^{q+1}}$$

if $q > k-2$. The ways of improving this lower bound on q have been discussed in [8].

In the general case, we set

$$G_m(k) = \sum_{m|i} \binom{k}{i}(-1)^i. \tag{5}$$

For example, for any prime p, we have $G_p(k) = 1$ for $0 \leq k < p$, and $G_p(p) = 0$. By identity (3), we get that

$$k!\, S(a\,(p-1)\,p^q, k) \equiv (-1)^{k+1} G_p(k) \pmod{p^{q+1}} \tag{6}$$

holds for all $q > 0$.

Now we are going to determine the generating function of $G_p(k)$ in identity (8) and deduce recurrence (9). An application of Lemma 7 to this recurrence will imply the required divisibility properties. For any odd m, we obtain

$$\begin{aligned}\sum_{k=0}^{\infty}\left[\sum_{m|i}(-1)^i\binom{k}{i}\right]x^k &= \sum_{m|i}(-1)^i\frac{x^i}{(1-x)^{i+1}}\\ &= \sum_{j=0}^{\infty}(-1)^{mj}\frac{x^{mj}}{(1-x)^{mj+1}}\\ &= \frac{1}{1-x}\left(1-\frac{(-x)^m}{(1-x)^m}\right)^{-1}\\ &= \frac{(1-x)^{m-1}}{(1-x)^m+x^m} = 1+x\frac{(1-x)^{m-1}-x^{m-1}}{(1-x)^m+x^m}.\end{aligned} \tag{7}$$

We note that an alternative derivation of identity (7) follows by binomial inversion [5].

From now on p denotes an odd prime. In some cases the discussion can be extended to $p = 2$, as will be pointed out.

We set $m = p$ and subtract 1 from both sides of (7), to yield

$$\sum_{k=1}^{\infty}G_p(k)x^k = x\frac{(1-x)^{p-1}-x^{p-1}}{(1-x)^p+x^p}. \tag{8}$$

We adopt the usual notation $[x^k]\,f(x)$ to denote the coefficient of x^k in the formal power series $f(x)$. If we multiply both sides of (8) by the denominator of the right-hand side and equate coefficients, we get a useful recurrence that helps us in deriving divisibility properties. Note that the right side is a polynomial of degree $p-1$. For $k \geq p$, we obtain that the coefficient of x^k is zero; i.e.,

$$[x^k]\left((1-x)^p+x^p\right)\sum_{i=1}^{\infty}G_p(i)x^i = 0.$$

It follows that

$$\sum_{i=0}^{p-1}(-1)^i\binom{p}{i}G_p(k-i) = 0,$$

i.e.;

$$G_p(k) = -\sum_{i=1}^{p-1}(-1)^i\binom{p}{i}G_p(k-i). \tag{9}$$

Remark: Note that for $p = 2$, identity (8) has a slightly different form as it becomes

$$\sum_{k=1}^{\infty} G_2(k)x^k = \frac{x}{1-2x},$$

and we can easily deduce that $G_2(k) = 2^{k-1}$ which agrees with $\nu_2(k!\,S(n,k)) = k-1$.

The calculation of $G_p(k)$ is more complicated for $p > 2$. However, we can find a lower bound on $\nu_p(G_p(k))$ and effectively compute $G_p(k) \pmod{p^{\nu_p(G_p(k))+1}}$ if $p-1 \mid k$ by making some observations about identity (9). We shall need the following general result:

Lemma 7: Let p be an arbitrary prime. Assume that the integral sequence a_k satisfies the recurrence

$$a_k = \sum_{i=1}^{d} b_i a_{k-i}, \quad k \geq d+1,$$

and that for some nonnegative integer m, $\nu_p(a_d) = m \geq 0$ and the initial values $a_i, i = 1, 2, \ldots, d-1$, are all divisible by p^m. Let $\nu_p(b_d) = r \geq 1$ and suppose that the coefficients b_i $(i = 1, 2, \ldots, d-1)$ are all divisible by p^r. We write $a_d = \alpha p^m$ and $b_d = \beta p^r$, and set $f(k) = f_p(k, m, r) = m + \left\lfloor \frac{k-1}{d} \right\rfloor r$. Then $\nu_p(a_k) \geq f(k)$, and equality holds if $d \mid k$. Moreover, for any integer $t \geq 1$, we have

$$a_{td} \equiv \alpha\beta^{t-1} p^{m+(t-1)r} \pmod{p^{m+tr}}.$$

According to the lemma, there is a transparent relation between the lower bound $f(k)$ on $\nu_p(a_k)$ and the parameters $\nu_p(a_d), \nu_p(b_d)$, and d provided $\nu(a_i) \geq m$ and $\nu_p(b_i) \geq r$ for $i = 1, 2, \ldots, d-1$.

We prove Lemma 7 in Section 5. With its help, we can now prove Theorem 1.

Proof of Theorem 1: By identity (5), we have $a_i = G_p(i) = 1$, for $i = 1, 2, \ldots, p-1$, and by identity (9), $b_i = (-1)^{i+1}\binom{p}{i}$ for $i = 1, 2, \ldots, p-1$; therefore, $\nu_p(a_i) = 0$ and $\nu_p(b_i) = 1$. We apply Lemma 7 with $d = p-1, m = 0, r = 1, \alpha = 1, \beta = -1$, and $s = 2$, and get

$$G_p(k) = a_k \equiv \begin{cases} (-1)^{\frac{k}{p-1}-1} p^{\frac{k}{p-1}-1} & \pmod{p^{\frac{k}{p-1}}}, \text{ if } k \text{ is divisible by } p-1, \\ 0 & \pmod{p^{\left\lfloor \frac{k}{p-1} \right\rfloor}}, \text{ otherwise.} \end{cases} \tag{10}$$

It follows that $\nu_p(a_k) \geq \frac{k}{p-1} - 1$, and equality holds if and only if $p-1 \mid k$. We define $\tau_p(k)$ by $\tau_p(k) = \nu_p(a_k) - \lfloor \frac{k-1}{p-1} \rfloor$. By identities (6) and (10), it follows that for all $q > \nu_p(a_k) - 1$, $\nu_p(k!\,S(n,k)) = \nu_p(a_k)$, which concludes the proof of Theorem 1. ∎

In the next two sections, we study the cases $p = 3$ and $p = 5$ in detail.

3. AN APPLICATION, $p = 3$

We set $m = p = 3$ and $\omega^3 = 1$. By identities (3) and (4), we have

$$\sum_{3|i} \binom{k}{i} (-1)^i = \frac{1}{3}\big((1-\omega)^k + (1-\omega^2)^k\big) = \frac{1}{3}(1-\omega)^k\big(1 + (1+\omega)^k\big). \tag{11}$$

Note that $1+\omega = -\omega^2$, and $(1-\omega)^2 = 1-2\omega+\omega^2 = -3\omega$. Therefore identity (11) implies

$$\sum_{3|i} \binom{k}{i} (-1)^i = \frac{1}{3}(1-\omega)^k\big(1 + (-\omega^2)^k\big) = \frac{1}{3}(-3\omega)^{k/2}\big(1 + (-\omega^2)^k\big). \tag{12}$$

For $6 \mid k$ we get $\frac{1}{3}(-3\omega)^{k/2}2 = (-1)^{k/2}2 \cdot 3^{k/2-1}$, yielding $\nu_3(k!\,S(n,k)) = k/2 - 1$ for $q > k/2 - 2$.

For k even and $3 \nmid k$, by identity (12) we have $(-1)^{k/2}3^{k/2-1}\omega^{k/2}(1 + \omega^{2k}) = (-1)^{k/2}3^{k/2-1}(\omega^{k/2} + \omega^{-k/2}) = (-1)^{k/2+1}3^{k/2-1}$, since $\omega^{k/2} + \omega^{-k/2} = \omega + \omega^{-1} = -1$ in this case.

We are left with cases in which k is odd. For k odd and $3 \nmid k$ we have two cases. If $k \equiv 1 \pmod 6$, say $k = 6l + 1$ for some integer $l \geq 0$, then by identity (11) we obtain $\frac{1}{3}(1-\omega)^{6l}(1-\omega)\big(1 + (-\omega^2)^{6l+1}\big) = \frac{1}{3}(-3\omega)^{3l}(1-\omega)(1-\omega^2) = (-3)^{3l} = (-3)^{\frac{k-1}{2}}$. If $k \equiv 5 \pmod 6$, say $k = 6l + 5$ for some integer $l \geq 0$, then by identity (11) we obtain $\frac{1}{3}(1-\omega)^{6l}(1-\omega)^5\big(1 + (-\omega^2)^{6l+5}\big) = \frac{1}{3}(-3\omega)^{3l}(1-\omega)^5(1-\omega) = \frac{1}{3}(-3)^{3l}(-3\omega)^3 = (-1)^{\frac{k+1}{2}}3^{\frac{k-1}{2}}$.

In summary, we get

Theorem 8: For $q > \left\lfloor \frac{k-1}{2} \right\rfloor - 1, k > 0$, and $k \not\equiv 3 \pmod 6$, we have

$$\nu_3(k!\,S(2a\,3^q, k)) = \left\lfloor \frac{k-1}{2} \right\rfloor.$$

Recall that if $k/3$ is an odd integer, then $\nu_3(k!\,S(n,k)) > q$ by Theorem 2.

4. AN APPLICATION, $p = 5$

For $p = 5$, we can use the fact that $G_5(k)$ can be expressed explicitly in terms of Fibonacci or Lucas numbers, with the formula depending on k modulo 20, as shown by Howard and Witt [6]. (The Fibonacci numbers F_n are given by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. The Lucas numbers L_n satisfy the same recurrence, but with the initial conditions $L_0 = 2$ and $L_1 = 1$.)

The power of 5 dividing a Fibonacci or Lucas number is determined by the following result [9]:

Lemma 9: For all $n \geq 0$ we have $\nu_5(F_n) = \nu_5(n)$. On the other hand, L_n is not divisible by 5 for any n.

Theorem 10: If $k \equiv 5 \pmod{10}$ then $G_5(k) = 0$. If $k \not\equiv 5 \pmod{10}$ then

$$\nu_5\big(G_5(k)\big) = \left\lfloor \frac{k-1}{4} \right\rfloor + \tau_5(k),$$

where

$$\tau_5(k) = \begin{cases} \nu_5(k+1), & \text{if } k \equiv 9 \pmod{20} \\ \nu_5(k), & \text{if } k \equiv 10 \pmod{20} \\ \nu_5(k+2), & \text{if } k \equiv 18 \pmod{20} \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

Proof: From a result of Howard and Witt [6, Theorem 3.2], we find that the value of $5^{-\lfloor (k-1)/4 \rfloor} G_5(k)$ is given by the following table:

$k \bmod 20$	0	1	2	3	4
$5^{-\lfloor (k-1)/4 \rfloor} G_5(k)$	$2L_{k/2}$	$F_{(k+1)/2}$	$F_{k/2+1}$	$L_{(k-1)/2}$	$L_{k/2-1}$

$k \bmod 20$	5	6	7	8	9
$5^{-\lfloor (k-1)/4 \rfloor} G_5(k)$	0	$-F_{k/2-1}$	$-L_{(k-1)/2}$	$-L_{k/2+1}$	$-F_{(k+1)/2}$

$k \bmod 20$	10	11	12	13	14
$5^{-\lfloor (k-1)/4 \rfloor} G_5(k)$	$-2F_{k/2}$	$-L_{(k+1)/2}$	$-L_{k/2+1}$	$-F_{(k-1)/2}$	$-F_{k/2-1}$

$k \bmod 20$	15	16	17	18	19
$5^{-\lfloor (k-1)/4 \rfloor} G_5(k)$	0	$L_{k/2-1}$	$F_{(k-1)/2}$	$F_{k/2+1}$	$L_{(k+1)/2}$

The result then follows easily from Lemma 9. ∎

We can now easily derive our main result on the divisibility of Stirling numbers by powers of 5.

Theorem 11: If n is divisible by $4 \cdot 5^q$, where q is sufficiently large, and $k \not\equiv 5 \pmod{10}$, then

$$\nu_5\big(k!\, S(n,k)\big) = \nu_5\big(G_5(k)\big) = \left\lfloor \frac{k-1}{4} \right\rfloor + \tau_5(k),$$

where $\tau_5(k)$ is given by (13).

Proof: Apply Lemma 5 to Theorem 10. ∎

Note that in Theorem 11 any q exceeding $\nu_5(k!\, S(n,k)) - 1$ will suffice; for instance, we can select the lower bound $\left\lfloor \frac{k-1}{4} \right\rfloor + \tau_5(k) - 1$.

Our proof of Theorem 10 does not generalize to other primes, so we mention another approach that in principle does generalize, though it is not easy to apply it to primes larger than 5.

The basic idea is to p-sect the generating functions $\sum_k G_p(k)x^k$. If $A(x) = N(x)/D(x)$, where $N(x)$ and $D(x)$ are polynomials, then we can determine all of the p-sections of $A(x)$ by multiplying the numerator and denominator of $A(x)$ by $D(\omega x)D(\omega^2 x)\cdots D(\omega^{p-1}x)$, where ω is a primitive pth root of unity: since $D(x)D(\omega x)\cdots D(\omega^{p-1}x)$ is invariant under substituting ωx for x, it must be a polynomial in x^p. For example, we find in this way that

$$\sum_{k=1}^{\infty} G_3(k)x^k = x\frac{(1-x)^2 - x^2}{(1-x)^3 + x^3} = \frac{x + x^2 - 3x^4 - 9x^5 - 18x^6}{1 + 27x^6} \tag{14}$$

and

$$\sum_{k=1}^{\infty} G_5(k)x^k = x\frac{(1-x)^4 - x^4}{(1-x)^5 + x^5} = \frac{N_5(x)}{1 + 5^4x^{10} + 5^5x^{20}}, \tag{15}$$

where

$$\begin{aligned} N_5(x) = {} & x + x^2 + x^3 + x^4 - 5x^6 - 20x^7 - 55x^8 - 125x^9 - 250x^{10} + 175x^{11} \\ & - 100x^{12} - 375x^{13} - 375x^{14} + 500x^{16} + 625x^{17} - 1250x^{19} - 2500x^{20}. \end{aligned} \tag{16}$$

Of course, once we have found these formulas, by whatever method, they may be immediately verified.

We note that in both of these generating functions the denominator is actually a polynomial in x^{2p} rather than just in x^p, and it is not difficult to show that this is true in general.

From (14) we can immediately derive a formula for $G_3(k)$. With somewhat more difficulty one can use (15) and (16) to determine the exact power of 5 dividing $G_5(k)$ and thereby give a different proof of Theorem 10.

5. THE PROOFS OF LEMMA 7, THEOREM 3, AND THEOREM 4

We present the proofs of some lemmas and theorems that were stated in Section 2.

Proof of Lemma 7: We prove that the following two assertions hold, by induction on k:

(i) $\nu_p(a_k) \geq f(k)$

(ii) If $k = td$, where t is a positive integer, then $a_k \equiv \alpha\beta^{t-1}p^{m+(t-1)r} \pmod{p^{m+tr}}$.

Note that (ii) implies that $\nu_p(a_k) = f(k)$.

If $1 \leq k \leq d$, then these assertions are consequences of the initial conditions. Now suppose that (i) and (ii) hold for $a_{k-d}, \ldots, a_{k-1}$. Then the induction hypothesis implies

that $b_i a_{k-i}$ is divisible by $p^{r+f(k-i)}$ for $i = 1, 2, \ldots, d$. We have $r+f(k-i) \geq r+f(k-d) = f(k)$, so $b_i a_{k-i}$ is divisible by $p^{f(k)}$, and thus so is $a_k = b_1 a_{k-1} + \cdots + b_d a_{k-d}$. This proves (i).

For (ii), suppose that $k = td$. By the induction hypothesis we have

$$a_{(t-1)d} \equiv \alpha \beta^{t-2} p^{m+(t-2)r} \pmod{p^{m+(t-1)r}}$$

and

$$\nu_p(a_{td-i}) \geq m + \left\lfloor \frac{td-i-1}{d} \right\rfloor r = m + (t-1)r, \quad \text{for } 1 \leq i < d.$$

Thus

$$b_d a_{(t-1)d} \equiv \beta p^r \cdot \alpha \beta^{t-2} p^{m+(t-2)r} = \alpha \beta^{t-1} p^{m+(t-1)r} \pmod{p^{m+tr}}$$

and

$$\nu_p(b_i a_{td-i}) \geq m + tr, \quad \text{for } 1 \leq i < d.$$

Then (ii) follows from the recurrence for a_k. ∎

We note that the lemma extends the study of situations discussed in [11] and [13] by relaxing the condition that the coefficient b_d be relatively prime to the modulus.

We can further generalize identity (10) and obtain the

Proof of Theorem 3: Analogously to the definition of (5), we set, for $0 \leq t \leq m-1$,

$$G_m(k,t) = \sum_{i \equiv t \pmod m} \binom{k}{i} (-1)^i.$$

In a manner similar to the derivation of identity (7), for every odd m, we obtain that

$$\sum_{k=0}^{\infty} \left[\sum_{i \equiv t \pmod m} (-1)^i \binom{k}{i} \right] x^k = \frac{(-x)^t (1-x)^{m-t-1}}{(1-x)^m + x^m}.$$

Note that the degree of the numerator is $m-1$. It is fairly easy to modify identities (8) and (9) for $G_m(k,t)$. An application of Lemma 7 to $G_p(k,t)$ yields Theorem 3. We note that here $\alpha = \binom{p-1}{t}(-1)^t$; hence $\alpha \equiv 1 \pmod p$. The congruence follows from the two identities, $\binom{p}{t} \equiv 0 \pmod p$, $\quad 1 \leq t \leq p-1$, and $\binom{p}{t} = \binom{p-1}{t-1} + \binom{p-1}{t}$. (We note that for every prime p and positive integer n, $\binom{p^n-1}{t} \equiv (-1)^t \pmod p$ also holds.) ∎

The interested reader may try another application of Lemma 7 to prove the following identity (cf. [1])

$$\nu_2\left(\sum_{k=0}^{n-1} \binom{2n-1}{2k} 3^k \right) = n-1, \quad n = 1, 2, \ldots.$$

Finally, we note that it would be interesting to find an upper bound on $\nu_p(a_k) - f(k)$ as a function of k. The case $p = 5$ and $k \equiv 9$, 10, or 18 (mod 20) shows that the difference can be as big as $C \log k$ with some positive constant C.

We conclude this section with the

Proof of Theorem 4: Theorem 3 deals with the case in which $m = 0$, thus we may assume that $m \geq 1$. Using the identities $i^m = \sum_{l=0}^{m} S(m,l)\binom{i}{l}l!$ and $\binom{k}{i}\binom{i}{l} = \binom{k}{l}\binom{k-l}{i-l}$ for $l \leq i \leq k$, we have

$$\begin{aligned}\sum_{i\equiv t \pmod p} \binom{k}{i}(-1)^i i^m &= \sum_{i\equiv t \pmod p} \binom{k}{i}(-1)^i \sum_{l=0}^{m} S(m,l)\binom{i}{l}l! \\ &= \sum_{l=0}^{m} S(m,l)\binom{k}{l}l! \sum_{i\equiv t \pmod p} \binom{k-l}{i-l}(-1)^i \qquad (17)\\ &= \sum_{l=0}^{m}(-1)^l S(m,l)\binom{k}{l}l! \sum_{i\equiv t-l \pmod p} \binom{k-l}{i}(-1)^i.\end{aligned}$$

Observe that Theorem 3 applies to the last sum.

We shall show that under the conditions of Theorem 4, the term with $l = m$ has the smallest exponent of p on the right side of (17). If $l = 0$ then $S(m,l) = 0$ in identity (17) so we need only consider the terms in which $l \geq 1$. Let $\chi_y(x)$ denote the indicator function of divisibility by y; i.e., $\chi_y(x) = 1$ if and only if $y \mid x$. We shall show that

$$\nu_p\left(\binom{k}{l}l!\, p^{\lfloor \frac{k-l}{p-1}\rfloor - \chi_{p-1}(k-l)}\right) = \nu_p(k!) - \nu_p((k-l)!) + \left\lfloor \frac{k-l}{p-1}\right\rfloor - \chi_{p-1}(k-l), 1 \leq l \leq m,$$

assumes its unique minimum at $l = m$; this fact, together with Theorem 3, implies Theorem 4.

By a well-known formula, we have

$$\nu_p((k-l)!) = \left\lfloor \frac{k-l}{p}\right\rfloor + \left\lfloor \frac{k-l}{p^2}\right\rfloor + \cdots.$$

The hypotheses of Theorem 4 imply that $k-m = r(p-1) \equiv -r' \pmod p$, where $1 \leq r' \leq p$ and $m \leq r'$. It follows that $\lfloor \frac{k-m+i}{p}\rfloor$ is constant for $i = 0, 1, \ldots, r'-1$; i.e., $\lfloor \frac{k-l}{p}\rfloor$ is constant for $l = m, m-1, \ldots, m-r'+1$. Since $r' \geq m$, this implies that $\lfloor \frac{k-l}{p}\rfloor$ is constant for $1 \leq l \leq m$. Similarly, $\lfloor \frac{k-l}{p^i}\rfloor$ is constant for $1 \leq l \leq m$. Therefore, $\nu_p\big((k-l)!\big)$ is constant for $1 \leq l \leq m$.

Next we show that

$$\left\lfloor \frac{k-l}{p-1}\right\rfloor - \chi_{p-1}(k-l) > \left\lfloor \frac{k-m}{p-1}\right\rfloor - \chi_{p-1}(k-m), \quad 1 \leq l < m. \qquad (18)$$

Since $p-1$ divides $k-m$, $k-l$ is not divisible by $p-1$ for $l = m-1, m-2, \ldots, m-p+2$, and since $m \leq p$, this implies all cases of (18) except $m = p, l = 1$. In this case we have

$$\left\lfloor \frac{k-1}{p-1} \right\rfloor - \chi_{p-1}(k-1) = 1 + \left\lfloor \frac{k-p}{p-1} \right\rfloor - \chi_{p-1}(k-p),$$

and thus (18) holds in this case also. The proof is now complete. ∎

We note that the generating function of the sum on the left hand side of (17) can be derived by binomial inversion [5] in terms of Eulerian polynomials.

6. CONJECTURES

Empirical evidence suggests that formulas for $\tau_p(k)$ exist based on the residue of k modulo $p(p-1)$. The following conjectures have been proved only in the cases $p = 3$ and $p = 5$.

Conjecture 1:

(a) If k is divisible by $2p$ but not by $p(p-1)$ then $\tau_p(k) = \nu_p(k)$.

(b) If $k+1$ is divisible by $2p$ but not by $p(p-1)$ then $\tau_p(k) = \nu_p(k+1)$.

Conjecture 2:

For each odd prime p, there is a set $A_p \subseteq \{1, 2, \ldots, p(p-1)-1\}$ such that if $k \not\equiv 0$ or $-1 \pmod{2p}$ and k is not an odd multiple of p, then $\tau_p(k) > 0$ if and only if k is congruent modulo $p(p-1)$ to an element of A_p.

It usually seems to be true that under the conditions of Conjecture 2, for each $i \in A_p$, there exists some integer $u_{p,i}$ such that if $k \equiv i \pmod{p(p-1)}$ then $\tau_p(k) \equiv \nu_p(k + u_{p,i})$.

For example, Theorem 7 asserts that the conjectures hold for $p = 3$, with $A_3 = \emptyset$, and Theorem 8 asserts that the conjectures hold for $p = 5$ with $A_5 = \{18\}$ and $u_{5,18} = 2$. Empirical evidence suggests that $A_7 = \{16\}$, with $u_{7,16} = 75$. Here are the empirical values of A_p for primes p from 11 to 23.

$A_{11} = \{14, 18, 73, 81, 93\}$

$A_{13} = \{82, 126, 148\}$

$A_{17} = \{37, 39, 62, 121, 179, 230, 234\}$

$A_{19} = \{85, 117, 119, 156, 196, 201, 203, 244, 279, 295, 299, 316, 320, 337\}$

$A_{23} = \{72, 128, 130, 145, 148, 170, 171, 188, 201, 210, 211, 232, 233, 234, 317, 325, 378, 466\}$

REFERENCES

1. D. M. Bloom. Solution to Problem 428. *College Math. Journal* **22** (1991): 257–259.

2. L. Comtet. *Advanced Combinatorics.* Dordrecht: D. Reidel, 1974.

3. R. Evans. "A congruence for a sum of binomial coefficients." Problem E2685. *Amer. Math. Monthly* **86** (1979): 130–131. Solution by H. F. Mattson, Jr.

4. A. Fleck. *Sitzungs. Berlin Math. Gesell.* **13** (1913–14): 2–6.

5. P. Haukkanen. "Some binomial inversions in terms of ordinary generating functions." *Publ. Math. Debrecen* **47** (1995): 181–191.

6. F. T. Howard and R. Witt. "Lacunary sums of binomial coefficients." *Applications of Fibonacci Numbers*, Vol 7: 185–195. Kluwer Academic Publishers, 1998.

7. H. Kapferer. "Über gewisse Summen von Binomialkoeffizienten." *Archiv der Mathematik und Physik* **23** (1915): 117–124.

8. T. Lengyel. "On the divisibility by 2 of the Stirling numbers of the second kind." *The Fibonacci Quarterly* **32** (1994): 194–201.

9. T. Lengyel. "The order of the Fibonacci and Lucas numbers". *The Fibonacci Quarterly* **33** (1995): 234–239.

10. A. Lundell. "A divisibility property for Stirling numbers." *J. Number Theory* **10** (1978): 35–54.

11. N. S. Mendelsohn. "Congruence relationships for integral recurrences." *Can. Math. Bull.* **5** (1962): 281–284.

12. J. Riordan. *An Introduction to Combinatorial Analysis.* New York: Wiley, 1958.

13. D. W. Robinson. "A note on linear recurrent sequences modulo m." *Amer. Math. Monthly* **73** (1966): 619–621.

AMS Classification Numbers: 11B73, 11B37, 11B50